IN THE CLAIMS

Please amend the claims as follows:

Claim 1-14 (Canceled).

Claim 15 (Currently Amended): A system for protecting a communication device against a denial-of-service attack, the system comprising:

a monitoring device ~~configured to be~~ provided on a local area network including ~~to which~~ the communication device ~~that is a target of the denial-of-service attack is connected~~, the monitoring device being configured to monitor ~~monitoring~~ a packet transmitted to the communication device via an internet-service-provider network; and

a restricting device ~~configured to be~~ provided on the internet-service-provider network, the restricting device being configured to restrict ~~restricting~~ a packet to the local area network, wherein the monitoring device includes

an attack detecting unit configured to detect ~~that detects~~ an attack by the packet on the communication device, and

a protection-request-information transmitting unit configured to transmit to the restricting device ~~that transmits~~ protection request information indicating a request for protection against the attack, the protection-request-information transmitting unit being configured to update the protection request information to exclude from restriction packets f not included in the attack, based on a report transmitted from the restricting device, ~~to the restricting device;~~ and

the restricting device includes a packet restricting unit configured to restrict ~~that restricts~~ a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

Claim 16 (Currently Amended): The system according to claim 15, wherein

the monitoring device further includes a signature generating unit <u>configured to</u>

<u>generate</u> ~~that generates~~ a signature indicating a feature of a packet that attacks the

communication device,

the protection-request-information transmitting unit transmits the protection request

information including the signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the signature.

Claim 17 (Currently Amended): The system according to claim 16, wherein

the restricting device further includes a signature determining unit <u>configured to</u>

<u>determine</u> ~~that determines~~ whether the protection request information including the signature

is appropriate, and

the packet restricting unit restricts a packet corresponding to a signature ~~that is~~

determined to be appropriate, and does not restrict a packet corresponding to a signature ~~that~~

~~is~~ determined to be inappropriate.

Claim 18 (Currently Amended): The system according to claim 16, wherein

the restricting device further includes

a report generating unit <u>configured to generate</u> ~~that generates~~ a report

including [[on]] a feature and an amount of <u>packets</u> ~~a packet~~ corresponding to the

signature, and a report transmitting unit <u>configured to transmit</u> ~~that transmits~~ the

report to the monitoring device, [[;]]

the signature generating unit generates a new signature based on the report,

the protection-request-information transmitting unit transmits the protection request

information including the new signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the new signature.

Claim 19 (Currently Amended): The system according to claim 18, wherein

the restricting device further includes a forwarding unit <u>configured to forward</u> ~~that~~

~~forwards~~ the protection request information to other restricting <u>devices</u> ~~device~~ provided on

the internet-service-provider network, [[and]] the forwarding unit ~~determines~~ <u>being</u>

<u>configured to determine</u> whether to forward the protection request information based on the

report generated by the report generating unit<u>,</u> ~~and forwards the protection request~~

~~information to the other restricting device upon determining that it is necessary to forward the~~

~~protection request information~~.

Claim 20 (Currently Amended): The system according to claim 17, wherein

the restricting device further includes a determination-result transmitting unit

<u>configured to transmit</u> ~~that transmits~~ a <u>determination</u> result ~~of determination~~ of the signature

determining unit to the monitoring device, ~~and when the result of determination indicates that~~

~~the signature is inappropriate,~~ the signature generating unit <u>of the monitoring device</u>

<u>generating</u> ~~generates, based on the result of determination,~~ a new signature indicating the

feature of the packet that attacks the communication device <u>when the determination result</u>

<u>indicates that the signature is inappropriate</u>.

Claim 21 (Currently Amended): A method of <u>causing a monitoring device and a</u>

<u>restricting device to protect</u> ~~protecting~~ a communication device against a denial-of-service

attack ~~using a monitoring device and a restricting device~~, the monitoring device being

~~configured to be~~ provided on a local area network <u>including</u> ~~to which~~ the communication

device ~~that is a target of the denial-of-service attack is connected~~ and <u>being configured to</u>

monitor ~~monitoring~~ a packet transmitted to the communication device via an internet-service-provider network, the restricting device being ~~configured to be~~ provided on the internet-service-provider network and being configured to restrict ~~restricting~~ a packet to the local area network, the method comprising:

detecting, at the monitoring device, an attack by the packet ~~attack detecting including the monitoring device detecting an attack by the packet~~ on the communication device;

transmitting, from the monitoring device to the restricting device, a ~~protection-request-information transmitting including the monitoring device transmitting~~ protection request information indicating a request for protection against the attack ~~to the restricting device~~; [[and]]

restricting, at the restricting device, packets ~~packet restricting including the restricting device restricting a packet~~ transmitted to the communication device via the internet-service-provider network based on the protection request information;

transmitting, from the restricting device to the monitoring device, a report including information on the attack; and

transmitting, from the monitoring device to the restricting device, an updated protection request information excluding from restriction packets not included in the attack, based on the report.

Claim 22 (Currently Amended): The method according to claim 21, further comprising:

~~signature generating including the monitoring device~~ generating, at the monitoring device, a signature indicating a feature of a packet that attacks the communication device, wherein

~~the protection request information transmitting includes transmitting the~~ protection request information transmitted to the restricting device includes ~~including~~ the signature ~~to the restricting device~~, and

~~the packet restricting includes restricting~~ a packet corresponding to the signature is restricted.

Claim 23 (Currently Amended): The method according to claim 22, further comprising:

~~signature determining including the restricting device~~ determining, at the restricting device, whether the protection request information including the signature is appropriate,

wherein ~~the packet restricting includes restricting~~ a packet corresponding to a signature ~~that is~~ determined to be appropriate is restricted, [[;]] and ~~not restricting~~ a packet corresponding to a signature ~~that is~~ determined to be inappropriate is not restricted.

Claim 24 (Currently Amended): The method according to claim 22, further comprising:

~~report generating including the restricting device~~ generating, at the restricting device, a report on a feature and an amount of packets ~~a packet~~ corresponding to the signature; and

~~report transmitting including the restricting device~~ transmitting the report from the restricting device to the monitoring device,

wherein ~~the signature generating includes generating~~ a new signature is generated at the monitoring device based on the report, ~~the protection request information transmitting includes transmitting the~~ protection request information including the new signature is transmitted to the restricting device, and ~~the packet restricting includes restricting~~ a packet corresponding to the new signature is restricted.

Claim 25 (Currently Amended): A computer-readable ~~recording~~ medium <u>storing</u> <u>thereon computer-readable instructions</u> ~~that stores a computer program~~ for protecting a communication device against a denial-of-service attack using a monitoring device and a restricting device, the monitoring device being ~~configured to be~~ provided on a local area network <u>including</u> ~~to which~~ the communication device ~~that is a target of the denial-of-service attack is connected~~ and <u>being configured to monitor</u> ~~monitoring~~ a packet transmitted to the communication device via an internet-service-provider network, the restricting device being ~~configured to be~~ provided on the internet-service-provider network and <u>being configured to</u> <u>restrict</u> ~~restricting~~ a packet to the local area network, ~~wherein the computer program causes a computer to execute~~ <u>the computer-readable instructions when executed by a computer cause</u> <u>the computer to perform the method comprising</u>:

~~attack detecting including the monitoring device~~ detecting<u>, at the monitoring device,</u> an attack by the packet on the communication device;

~~protection-request-information transmitting including the monitoring device~~ transmitting<u>, from the monitoring device to the restricting device,</u> protection request information indicating a request for protection against the attack ~~to the restricting device~~; [[and]]

~~packet restricting including the restricting device~~ restricting<u>, at the restricting device,</u> a packet transmitted to the communication device via the internet-service-provider network based on the protection request information<u>;</u>

<u>transmitting, from the restricting device to the monitoring device, a report including</u> <u>information on the attack; and</u>

transcribing, from the monitoring device to the restricting device, an updated

protection request information excluding from restriction packets not included in the attack,

based on the report.

Claim 26 (Currently Amended): The computer-readable ~~recording~~ medium according

to claim 25, <u>further comprising:</u> ~~wherein~~

~~the computer program further causes the computer to execute signature generating~~

~~including the monitoring device~~ generating, <u>at the monitoring device,</u> a signature indicating a

feature of a packet that attacks the communication device<u>;</u> [[,]]

~~the protection request information transmitting includes~~ transmitting<u>, from the</u>

<u>monitoring device to the restricting device,</u> the protection request information including the

signature<u>;</u> ~~to the restricting device,~~ and

~~the packet restricting includes~~ restricting<u>, at the restricting device,</u> a packet

corresponding to the signature.

Claim 27 (Currently Amended): The computer-readable ~~recording~~ medium according

to claim 26, <u>further comprising:</u> ~~wherein~~

~~the computer program further causes the computer to execute a signature determining~~

~~procedure of determining including the restricting device~~ determining<u>, at the restricting</u>

<u>device,</u> whether the protection request information including the signature is appropriate<u>;</u> [[,]]

~~the packet restricting includes~~ restricting a packet corresponding to a signature ~~that is~~

determined to be appropriate ~~by the signature determining unit, which is to be transmitted to~~

~~the communication device~~; and

not restricting a packet corresponding to a signature ~~that is~~ determined to be

inappropriate~~, which is to be transmitted to the communication device~~.

Claim 28 (Currently Amended): The computer-readable ~~recording~~ medium according to claim 26, <u>further comprising:</u> ~~wherein~~

~~the computer program further causes the computer to execute:~~

~~a report generating procedure of generating including the restricting device~~ generating<u>, at the restricting device,</u> a report on a feature and an amount of <u>packets</u> ~~a packet~~ corresponding to the signature; and

~~a report transmitting procedure of transmitting including the restricting device~~ transmitting the report <u>from the restricting device</u> to the monitoring device<u>;</u> [[,]]

~~the signature generating procedure includes~~ generating<u>, at the monitoring device,</u> a new signature based on the report<u>;</u> [[,]]

~~the protection-request-information transmitting procedure includes~~ transmitting<u>, from the monitoring device to the restricting device,</u> the protection request information including the new signature<u>;</u> ~~to the restricting device,~~ and

~~the packet restricting procedure includes~~ restricting<u>, at the restricting device,</u> a packet corresponding to the new signature~~, which is to be transmitted to the communication device~~.